SUBMISSION TO THE PRESIDENT'S IDENTITY THEFT TASK FORCE

19 January 2007

The Honorable Alberto R. Gonzales
Attorney General
United States of America
Department of Justice
Washington, D.C. 20530

The Honorable Deborah Platt Majoras
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Attorney General Gonzales and Chairman Majoras:

As the Federal Identity Theft Task Force finalizes its strategic plan for President Bush, I would like to provide some recommendations in response to the Task Force's recent call for comments. My suggestions are based on more than a decade of experience in senior executive leadership positions of a security industry pioneer that invented some of the core security technologies that protect the Internet. Over the years, I have had an opportunity to see the very best of what the technology industry can do to protect the sensitive information of consumers as well witness the emergence of a complex and ever-changing threat environment in cyberspace.

ID theft, of course, is not limited to the online world and I know very well that the Task Force clearly understands that. I also know that under your leadership, the President's Identity Theft Task Force recognizes that cyber-crime is one of the fastest growing threats to consumers' identities and information. Through the various forms of online fraud – from "spear" and "puddle" phishing to utilize social engineering techniques to the use of hi-jacked Trojans to steal information on a user's computer system, there are a range of techniques and tools criminals use to feed an ecosystem in cyberspace that thrives on stolen information and identities of individuals and organizations.

The Task Force is right in addressing the overall issue of Identity Theft – including the online component – by looking at ways to enhance data protection for sensitive consumer information, improve coordination and the effectiveness of criminal prosecution to identity theft, and to provide achievable guidance to both the business community and businesses to address this growing menace to our society and economy. In addition, I believe that the Task Force also has an obligation to make recommendations that will:

1) *Encourage organizations in the private and public that hold sensitive information on consumers to understand what the risks are to that information.*

2) *Provide guidance to organizations that once they understand the risks to the sensitive information of consumers, that information must be properly managed and secured.* Effective preventative measures or security safeguards should be deployed to protect such information. If that information is breached, it should be rendered unusable or unreadable by an unauthorized third party.

3) *Allow consumers to know when their information is at risk, which could either lead to identity theft or some other type of fraud that could result in actual harm*. Consumers should be notified by organizations if that information and their identities have been put at risk.

The good news is that there are initiatives in both the public and private sectors that can be utilized as potential models or examples of how to address these additional recommendations. They include:

- The Federal Financial Services Examination Council (www.ffiec.org) issued strong guidance in October 2005 (http://www.ffiec.gov/press/pr101205.htm) that directed financial institutions offering online services to: 1) conduct a risk assessment, 2) put measures in place that were stronger than a static password to address those risks, and 3) educate consumers on the risks to their identities and information and what practices and tools are available to address those risks. The October 2005 guidance was issued after a comprehensive study of the problem of Online Account Hi-jacking and what could be done by banks to address it effectively. That guidance, entitled "Authentication in an Internet Banking Environment" has spurred the marketplace to better understand risks to consumer online banking and what could be done to provide security safeguards that more effectively protect consumers' identities and information.

- Industry standards and frameworks continually evolve to address emerging threats to consumers' sensitive information. To address online threats, there are widely accepted best practices that can be utilized in providing guidance on effective safeguards to protect that information and consumers' identities. The Payment Card Industry Standard (PCI) is one such framework: https://www.pcisecuritystandards.org/ I highly recommend that the Task Force encourage organizations to adopt proven safeguards that will help prevent breaches from occurring in the first place. There is no "silver bullet," but there are a series of steps that an organization can take to assess its risk, establish an information security policy, put proven practices in place that protect that information and then enforce those policies. PCI is one such framework.

- I strongly support a national breach notification regime. There now 35 state breach notification laws that have been enacted in the U.S. and that provides too much complexity for businesses, uncertainty for consumers and the risk of uneven enforcement. The U.S. should have a national breach notification law that incents

organizations to adopt reasonable security practices that help prevent breaches, with both state AG and federal enforcement.

- In a meeting with Assistant Secretary Garcia of Homeland Security, I strongly endorsed his plan to implement the President's *Strategy to Secure Cyberspace* that was issued in 2003. Coordination with his office could only enhance your efforts.
- In Section I of the Task Force's report, it discusses the potential need to further educate businesses and consumers on how they can safeguard their information and follow certain best practices. I believe that education and awareness is an important component to decreasing ID theft. That said, I urge the Administration to continue to support private-public partnerships, such as the National Cyber Security Alliance, a 501(c)3 non-profit organization designed to educate consumers, businesses, K-12 and higher education audiences on how they can stay safe online and protect their information. By combining industry and government resources, the public and private sector can work together to solve these important issues and better educate all audiences and stakeholders.

As a leading provider of anti-fraud intelligence and leading information security solutions, some might expect me to come out in favor of heavy regulation that would force organizations to adopt security solutions. To the contrary, I think that the Bush Administration and the U.S. Congress need to be flexible as possible as these problems are addressed. However, government does have a role to play in helping to protect sensitive consumer information, and in addition to strong enforcement and education, government should push organizations to understand what their risks are, to adopt the appropriate measures that will address those risk (and to enable flexibility as the threats evolve), and government should also see to it that consumers are notified when their information and identities are at risk.

Sincerely,

Arthur W. Coviello, Jr.
President, RSA – The Security Division of EMC Corporation

Cc: Shannon Kellogg, Director of Information Security Policy, EMC Government Affairs